REMARKS

Reconsideration and allowance of the claims pending in the application are requested.

Claims 1 – 28 are pending in the application.

Claims 1 – 4 have been rejected under 35 USC 102(e) as anticipated by USP 6,212,549 to J. D. Page et al, issued April 3, 2001, filed October 1, 1998 (Page).

Claims 5-7, 12-15, 17 and 23 have been rejected under 35 USC 102 (b) as anticipated by USP 5,768, 586 to M. Zweben et al, issued June 16, 1998 (Zweben).

Claims 24-28 have been rejected under 35 USC 102(e) as anticipated by USP 6,237,097, to Y. Frankel et al, issued May 21, 2001, filed May 22, 1999 (Frankel).

Claims 8, 9, and 11 have been rejected under 35 USC 103 (a) as unpatentable over Zweben, of record in view of USP 6,549,210 to Van Hook, of record.

Claims 10 and 18 have been rejected under 35 USC 103 (a) as unpatentable over Zweben, of record in view of USP 6,662,167 to Xiao, of record.

Claims 16 and 19-21 have been rejected under 35 USC 103 (a) as unpatentable over Zweben, of record in view of USP 5,768,385 to Simon, of record.

Claim 22 has been rejected under 35 USC 103 (a) as unpatentable over Zweben, of record in view of USP 5,768,385 to Puhl, of record.

Applicants have amended claims 1, 3 and 5 to further distinguish the present invention (Jakobsson) from the cited art.

Before responding to the rejections, applicants would like to distinguish Page, Zweben and Frankel and the combination of Zweben with Van Hook, Xiao and Simon from the present invention (Jakobsson), as follows:

1. USP 6,212,549 to Page discloses a computer-implemented method for facilitating collaboration and communication among project participants working collaboratively on a project using a computer network. A plurality of trackpoints that are created by at least two of the project participants. Each of the plurality of trackpoints includes metadata descriptive of the each of the plurality of trackpoints. Each of the plurality of trackpoints is configured to store data within its content. Indices of trackpoints are provided based on searchable keys. A plurality of

tools are provide and include at least one of a search tool, a notification tool, and a briefing book page, the search tool being configured to search the indices for at least one trackpoint of the plurality of trackpoints that satisfies search criteria, the notification tool being configured to notify a project participant that is authorized to use the notification tool when notification criteria are satisfied, and the briefing book page represents a data presentation mechanism that is configured to receive briefing book data from at least two of the plurality of trackpoints. Page fails to disclose the limitations of Jakobsson, as follows:

A. Page discloses a computer implemented project management system using trackpoints for tracking tasks in development projects. Page fails to disclose a Proof Of Work (POW) as a computational task performed in a specified time interval to accomplish a separate, useful and verifiably correct computation for data security applications.

B. Page discloses assigning security classifications to trackpoints for restricting trackpoint access. Page fails to disclose a POW in a data security application protocol convincing a verifier that a prover possesses knowledge of a secret.

C. Page discloses creating trackpoints to facilitate tracking events/items pertaining to a project, i.e. manufacturing, development, etc. Page fails to disclose an entity distributing a computational task among a plurality of sub-entities, each entity performing a POW which are assembled as a response to the entity in a data security application protocol.

D. Page discloses assigning security classifications to trackpoints in a project. The classifications limiting a project participant viewing project management data. Page fails to disclose recycling a POW_1 to supplement a POW_2 in convincing an entity to accept its POW_2 in a data security application protocol.

2. USP 5768586 to Zweben discloses modeling of an enterprise. A model developer uses a high-level modeling language to describe the enterprise with constructs that are more readily accessible to the model developer than those used in other previous modeling languages.

The high-level description is translated into a low-level description that can more readily be used by a processing device to dynamically exercise the model. The constructs of the modeling language shield the model developer from many of the mundane tasks associated with maintaining data integrity in complex data structures. The modeling language includes data constructs that make it easy to track and maintain data that changes during execution of a program, without considerable effort on the part of the model developer. These data constructs can be used to restore various states of the modeled enterprise during execution of the program, either automatically or at the direction of a user, and can be used to develop a scheduling system for scheduling a complex activity and revising the schedule as necessary to accommodate changed circumstances. Zweben fails to disclose the limitations of Jakobsson, as follows:

A. Zweben discloses dynamically modeling an enterprise, each state of the enterprise being modeled by a set of configuration data subject to one or more operations changing the state of the model. Zweben fails to disclose minting coins based on a k-way hash function collision where a computationally entity is instructed to look within a pre-defined search space for "k" l-bit pre-images that hash to a range of y of l-bit images whose "t" least significant digits have the value "s" , where for security purposes, l is very large.

B. Zweben discloses storing context data for each operation, the data representing changes between configuration data before and after an operation and establishing a current set of configuration data after the operation. Zweben fails to disclose a plurality of computational entities, each generating a reply as a POW_1 which will be an l-bit pre-image that hashes to an l-bit image within a pre-defined range, and used by an entity 2 to achieve acceptance of POW_2 by entity 1.

3. USP 6,237,097 to Frankel discloses robust efficient distributed generation of RSA keys. An efficient protocol is one which is independent of the primality test "circuit size", while a robust protocol allows correct completion even in the presence of a minority of arbitrarily misbehaving malicious parties. The disclosed protocol is secure against any minority of malicious parties (which is optimal). The disclosed method is useful in establishing sensitive distributed cryptographic function sharing services (certification authorities, signature schemes

with distributed trust, and key escrow authorities), as well as other applications besides RSA (namely: composite ElGamal, identification schemes, simultaneous bit exchange, etc.). The disclosed method can be combined with proactive function sharing techniques to establish the first efficient, optimal-resilience, robust and proactively-secure RSA-based distributed trust services where the key is never entrusted to a single entity (i.e., distributed trust totally "from scratch"). The disclosed method involves new efficient "robustness assurance techniques" which guarantee "correct computations" by mutually distrusting parties with malicious minority. Frankel fails to disclose the limitations of Jakobsson, as follows:

A. Frankel discloses an electronic method for generating shares of a cryptographic value wherein participants perform first, second and third protocols to compute shares of the cryptographic value without revealing the cryptographic value to the participants and to detect whether a participants has deviated from a protocol. The distribution in Frankel et al (as in most cryptographic protocols) is such that if the "wrong" participants obtain a request to perform computation, then the computation cannot be performed. Similarly, once the system has been set up, the party that distributes computational requests needs the cooperation of a sufficient number of servers from a pre-selected set.

In contrast, any server can perform computation in the Jakobsson protocol. This includes the server that distributes the requests were the server not to find any cooperative servers to help it. It could also let one or more servers that it has not performed any previous exchange or setup of secrets do it. Frankel fails to disclose distributing a task to any server that can perform computation in the protocol.

Summarizing, Page fails to disclose a Proof Of Work (POW) as a computational task performed in a specified time interval to accomplish a separate, useful and verifiably correct computation for data security applications. Zweben fails to disclose minting coins based on a k-way hash function collision where a computationally entity is instructed to look within a pre-defined search space for "k" l-bit pre-images that hash to a range of y of l-bit images whose "t" least significant digits have the value "s" , where for security purposes, l is very large. Frankel

fails to disclose a POW where any server can perform computation in the protocol. The rejection of claims 1 – 28 under 35 USC 102 (b), and (e) is without support in the cited art for the reasons described above. Withdrawal of the rejection and allowance of claims 1 – 28 are requested.

Now turning to the rejection, applicants respond to the indicated paragraph of the Office Action, as follows:

Paragraphs 1-4:

The Examiner's comments are noted.

Paragraphs 5:

Claims 1-4 include limitations not disclosed in Page, as follows:

a. Claim 1:

(i) "distributing a computational task among a plurality of entities for execution within a specified interval of time, as a POW"

Page, at col. 6, lines 21-46, discloses a track point data base including track points created by project participants to facilitate tracking events/items pertaining to a project. A track point is represented by meta data, which describes the track point as a whole. The meta data may also include key words, subject, abstract and other descriptive and/or bibliographic data pertaining to the track point. Accordingly, the track point is not a computational task or distributed among entities for execution within a specified interval of time, as a proof of work (POW).

(ii) "receiving the POW relating to said task from one of said pluralities entities and using said POW to accomplish said task."

A track point enables a project participant to conduct full searches so that the attribute identifies track points of interest. Col. 8, lines 16-22. Track points do not receive a POW or use the POW to accomplish a task.

Page fails to disclose the limitations of claim 1. The rejection of claim 1, based on the cited art is without support.

b. Claim 2:

(i) "using said POW to accomplish a security goal."

Page, at col. 9, line 65 through col. 10, line 11 discloses the security classification is assigned to a track point to restrict track point access. In contrast, Jakobsson, at page 7, lines 11-12 discloses using a POW in security protocols.

Page fails to disclose a POW or using a POW to accomplish a security goal.

c. Claim 3:

Page fails to disclose the computational task or partitioning the task into a plurality of sub-task for distribution to one of a plurality of entities. In any case, claim 3 depends upon claim 1 and is patentable on the same basis as claim 1.

d. Claim 4:

Claim 4 depends upon claim 1 and is patentable on the same basis as claim 1.

Regarding Paragraph 6:

Claims 5-7, 12-15, 17 and 23 include limitations not disclosed in Zweben, as follows:

a. Claim 5:

(i) "partitioning a minting operation into a plurality of sub-computation tasks;"

Zweben, at col. 5, lines 20-49, discloses a prior art method of developing a computer module to aid in managing an organizational enterprise. Applicants can find no disclosure in Zweben relating to the claimed limitations of partitioning a minting operation into a plurality of subtask; receiving a POW from an entity and using the POW to accomplish a mini-operation, as described in the specification, at page 10, lines 6-12 and at page 1, lines 11-13.

The rejection of claim 5 is without support in the cited art.

b. Claim 13:

(i) "distributing a minting operation among a plurality of entities in a manner that maintains privacy in said minting operation;"

Claim 13 further describes a minting operation and is patentable on the same basis as claim 5.

c. Claims 6 & 14:

(i) "using said POW to accomplish a security goal..."

Zweben, at col. 6, lines 8-26, discloses a system and method used to create a scheduling module that implements a scheduling technique as constraint-based iterative repair. Zweben fails to disclose a POW or a POW offering a security goal.

d. Claim 7, 12, 15:

(i) "said minting operation includes identifying valid solutions that hash to a predetermined image and wherein said POW represents a valid solution."

Zweben, at col. 21, lines 32-48, discloses a context as a group of hash tables, which enable the state of all of the program data values to be tracked and maintained. Zweben fails to disclose a hash function occurs within a predefined search space and a range of images, as described in the specification at page 11, lines 9-12.

e. Claim 17:

(i) "said predetermined number of valid solutions hash to a portion of said target value."

Zweben, at col. 21, lines 32-48 discloses the "context" stores information regarding any change in the configuration of the program, after the point at which the context was opened. The cited text does not describe or suggest hashing valid solutions to a portion of a target value. In any case, claim 17 depends upon claim 15 and is patentable on the same basis. As claim 15

f. Claim 23:

(i) "The method of claim 13 further comprising verifying said POW."

Zweben at col. 6, lines 8-26, disclose a scheduling system for scheduling an activity. A scheduling model implements a scheduling technique known as constraint-based iterative repair. The schedule that does not satisfy constraints is modified to obtain a series of schedules until all of the modified schedules satisfies the constraints. The cited text does not describe a POW or verifying a POW.

Summarizing, claims 5-7, 12-15, 17 and 23 describe a minting operation using a POW distributed and partitioned into sub-tasks. Zweben discloses a prior art method of developing a computer module to aid in managing an organizational enterprise. Zweben fails to disclose a minting operation. Without support in the reference, the rejection does not satisfy the requirements of 35 USC 102(b).

Regarding Paragraph 7:

Claims 24-28 include limitations not disclosed in Frankel, as follows:

a. Claim 24:

(i) "generating a computational task for a certain amount of intense computation in a specified period of time as a POW to accomplish a separate useful and verifiable correct computation"

Frankel, at col. 10, lines 38-48, discloses servers generating and verifying randomized polynomials for verifying shares in a secret key assembled by a group of computers. All servers having to check shares to see whether local server shares match public shares. The cited text does not describe generating a POW to accomplish a separate, useful and verifiable correct computation.

(ii) "distributing the computational task for execution among a plurality of server entities;"

Frankel, at col. 10, lines 49-67, describes proving correctness of verification shares. Each server generates random polynomials. The server distribute the shares in these polynomials and broadcasts verification shares. Each server verifies its received polynomial shares, and the

received verification shares. Col. 10, lines 13-25. The cited text discloses a verification operation and not a computational operation.

(iii) "receiving a POW relating to said task from one of said plurality of said server entities; and

Frankel fails to describe receiving a POW relating to said task from one of said plurality of server entries.

(iv) "using said POW to verify and accomplish said computational task."

Frankel, at col. 10, lines 49-67, describes proving the correctness of verification shares. Frankel discloses verifying secret shares with verification shares and fails to disclose a POW by which a prover demonstrates to a verifier that a certain amount of computation work has been performed in a specified interval of time. The matching of secret shares and verification shares does not disclose or suggest a POW accomplishing a computational task. Frankel does not disclose or suggest using a POW to accomplish a computational task for a minting operation which minimizes effort by reusing POWs.

Frankel fails to disclose the limitations of claim 24, as described above and without such disclosure, there is no support for the rejection of claim 24 under 35 US 102(e). Withdrawal of the rejection and allowance of claim 24 are requested.

b. Claim 25:

Frankel, at col. 12, line 51 to col. 13, line 29, describes proof of knowledge of corresponding representations where a prover proves that it knows the values of corresponding representations. The cited text does not describe or suggest a POW having a hardness by a Prover and Verifier performing coin flips of at most w steps of computation in a time interval,. Claim 25 further limits claim 24 and further distinguishes claim 24 from the cited art. Withdrawal of the rejection and allowance of claim 25 are requested.

c. Claim 26:

Frankel, at col. 13, line 60 to col. 14, line 19, describes determining whether a previously computed value N is the product of two prime numbers. Frankel does not disclose determining if a proof of work is feasible if a Prover with an average of w computation steps in a time interval can cause a Verifier to the proof within a probability p. Frankel does not address the problem of identifying a feasible proof of work, but is directed to verifying shares of a secret key.

d. Claim 27:

Frankel, at col. 13, lines 60 to col. 14, line 19, fails to disclose the limitations of claim 27 on the same basis as the cited text failed to describe or suggest claim 26.

e. Claim 28:

Frankel, at col. 14, line 37 to col. 15, line 22, describes key generations for small public key. The cited text does not describe a POW or an efficient POW which reduces the work of a verifier by re-cycling POWs.

Summarizing, claims 24-28 relate to qualities of POWs whereas Frankel is directed to RSA key generation. The rejection of claims 24-28 under 35 USC 102e is without support in the cited art.

Regarding Paragraph 8:

Claim 8, 9 and 11 include limitations not disclosed or suggested in Zweben in view of Van Hook, of record, as follows:

a. Claims 8 & 9:

(i) "The method of claim 6 wherein said predetermined image comprises a range of images. and wherein all images within said range of images have a predetermined number of least significant bits in common.

Van Hook does not supply the missing elements in Zweben. **Van Hook appears to use hash functions of a different type than is used in cryptography. There are two types of computation known as hashing. The one that Van Hook relates to is not collision resistant,**

and is not hard to invert. The Jakobsson hash functions are collision resistant and hard to invert. Van Hook cannot practice his invention with a cryptographic hash function. To do so, would render his technique meaningless. Whereas Jakobsson could distribute any type of hashing Function. Moreover, finding partial hash collisions is not meaningful in the context of hash functions of the type disclosed by Van Hook.

In particular, Van Hook, at col. 9, lines 55-67, discloses hashing an index of coordinate values descriptive of an image where the hashed index value is used to map the memory locations in main memory. The locations are referred to by (s) "and (t) coordinates". The hashed index enables coordinates varying in only a few bits to be mapped to different locations in a cache memory. In contrast, Applicants, at pg. 11, lines 8-12, disclose an entity transmits a hash function to be used in identifying collisions within a predefined search space for pre-images that have a range of images whose "t" least significant bits have the value "s". Van Hook hashes an index of coordinates for an image location and fails to disclose hashing the coordinates of a range of images that map to a single image.

Van Hook, at col. 11, line 13-25, discloses a process for cache index hashing for an (s) coordinate that is fed into first and second portions on a (t) address is fed into first and second portions. The division of coordinates can be based on some number that most or least significant bits or any other suitable scheme. The cited text does not disclose or suggest images within a range of images have a predetermined number of least significant bits in common.

Summarizing, applicants describe a linking operation that identifies valid solutions that hash to a range of images for a predetermined image. Van Hook does the opposite of Jakobsson by reducing the likelihood that adjacent addresses will match the map to the same cache region. Moreover, the Examiner has not demonstrated in any respect a motivation or reasonable expectation of success in combining Van Hook with Zweben to implement a computational effort invested in a proof of work for accomplishing a minting operation. Finally, Zweben and Van Hook fail to disclose all of the limitations of claim 8 and 9.

The rejection of claims 8 and 9, under 35 USC 103(a) is not supported in the cited art. Withdrawal of the rejection and allowance of claims 8 and 9 are requested.

b. Claim 11:

Claim 11 further limits claims 5 and 6 in overcoming the rejection under 35 USC 103 (a)., and is patentable on the same basis thereof.

Regarding Paragraph 9:

Claims 10 and 18 include limitations not disclosed or suggested in Zweben, in view of Xaio, of record, as follows:

a. Claims 10 & 18:

Xiao does not supply the missing limitations in Zweben. Xiao, at col. 2, lines 26-53 discloses the parameters for real-world scheduling/sequencing to accommodate different conditions and able to adapt to changes. Applicants can find no disclosure in Xiao relating to searching a different solution search space for valid solutions, as described in the specification at pg. 11, line 20 continuing to pg. 12, line 5. The scheduling/sequencing problems and evolutionary computation used in resolving those manufacturing scheduling problems, does not disclose or suggest sub-task searching different solution search space for valid solutions. Without such disclosure, there is no basis for a worker skilled in the art to implement claims 10 and 18. the rejection of claims 10 and 18 under 35 USC 103(a) fails for lack of support in the prior art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested

The motivation to modify Zweben by the teachings of Xiao to produce a near optimal or optimal sequence of products for manufacture does not enable a worker skilled in the art to implement a minting operation in a computational effort invested in a POW. The rejection of claims 10 and 19, based on 35 USC 103(a) is without support in the cited art. Withdrawal of the rejection and allowance of claims 10 and 18 are requested. Regarding Paragraph 10:

Claims 16 and 19-21 includes limitations not disclosed in Zweben, in view of Simon, as follows:

a. Claims 16 & 19-21:

Simon fails to disclose the missing limitations in Zweben. Simon, at col. 8, lines 65 to col. 9, line 15, discloses public keying encryption and the use of message authentication codes to ensure that messages between parties are not tampered with by someone other than the sender. Applicants can find no disclosure in Simon relating to using a suitable hash function and string concatenation, including a secret value, for generating a coin to be minted, as described in the specification at pg. 13, lines 3-14.

A worker skilled in the art would not be motivated to modify Zweben with Simon to implement a method of accomplishing a minting operation using a computational effort invested in a POW. Without such motivation or reasonable expectation of success, and the failure of the cited references to describe all of the claim limitations, there is no basis under 35 USC 103(a) for the rejection of claim 16 and 19-21.

Withdrawal of the rejection and allowance of claims 16 and 19-21 requested.

Regarding Paragraph 11:

Claim 22 includes limitations not disclosed in Zweben, in view of Puhl, of record, as follows:

Puhl fails to disclose the missing limitation in Zweben. Puhl, at col. 17, lines 24-42, discloses storing secret keys and member certificates in a wireless identity module software token. The member keys are protected by passphrase information. The information is concatenated with a secret value for the device and run through a secure hash in order to generate encryption/encryption key for use in protecting the user's private key. In contrast, applicants at page 13, lines disclose a hash function is concatenated with a secret value "r" specific to each coin to be minted. The computation performed aids in the successful completion of the task of finding the requisite number of pre-image values that hash to a specific range of images for the purpose of minting coins. Puhl discloses hashing for generating encryption/encryption keys and not for the purpose of minting coins.

A worker skilled in the art would not be motivated to modify a method of modeling an enterprise, via a wireless electronic commerce system, to implement a minting operation having privacy using a hash operation and a secret value. Further, the Examiner has not demonstrated any reasonable expectation of success for such a combination to implement the method of claim 22. The rejection of claim 22 is without support in the cited art. Withdrawal of the rejection and allowance of claim 22 are requested.

CONCLUSION:

Having amended claims 1, 3, 5 to further distinguish the claims from the prior art, Applicants request entry of the amendment, allowance of the claims and passage to issue of the case.

AUTHORIZATION:

The Commissioner is hereby authorized to charge any additional fees which may be required for consideration of this Amendment to Deposit Account No. 13-4503, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

In the event that an extension of time is required, or which may be required in addition to that requested in a petition for an extension of time, the Commissioner is requested to grant a petition for that extension of time which is required to make this response timely and is hereby authorized to charge any fee for such an extension of time or credit any overpayment for an extension of time to Deposit Account No. 13-4503, Order No. JAKOBSSON 23-5 (3037-4196). A DUPLICATE OF THIS DOCUMENT IS ATTACHED.

Respectfully submitted,

MORGAN & FINNEGAN, L.L.P.

Dated: June 6, 2005 By: Joseph C. Redmond, V

Joseph C. Redmond, Jr., Reg. No. 18,753
Telephone: (202) 857-7887
Facsimile: (202) 857-7929

CORRESPONDENCE ADDRESS:

Morgan & Finnegan L.L.P.
3 World Financial Center
New York New York